AMENDMENTS TO THE CLAIMS

The following is a complete, marked-up listing of revised claims with a status identifier in parenthesis, underlined text indicating insertions, and strike through and/or double-bracketed text indicating deletions.

LISTING OF CLAIMS

1.   (Currently Amended)   A method for signing access operations to electronic data, comprising:

performing a security check upon each access operation in order to ascertain the identity of a user;

assigning a user signature, identifying the user, on the basis of the performed security check without being viewable by the user;

assigning at least one role signature, each role signature being assignable to a plurality of users, on the basis of the performed security check without being viewable by the user, each role signature identifying a different activity group with a particular responsibility;

signing each access operation to electronic data by specifying the user signature and the at least one role signature; and

recording each access operation [[and]] by storing, in an audit memory, accessed data information and access operation information together with the user signature and the at least one role signature specified for each access operation, wherein

each access operation is recorded in an audit memory,

the user signature is recorded in a user signature memory and in the audit memory, and

the at least one role signature is recorded in a role signature memory and in the audit memory.

2.   (Original)   The method as claimed in claim 1, wherein the security check involves biometric data from the user being ascertained.

3.   (Original)   The method as claimed in claim 1, wherein the security check involves reading at least one of an electronic and mechanical key.

4.   (Previously Presented)   The method as claimed in claim 1, wherein the user signature to be assigned is ascertainable on the basis of the data ascertained in the security check, by checking the user signature memory.

5.   (Previously Presented)   The method as claimed in claim 1, wherein the at least one role signature to be assigned is ascertainable on the basis of the data ascertained in the security check, by checking the role signature memory.

6.   (Original)   The method as claimed in claim 4, wherein the user signature memory is checked using a data telecommunication link.

7.   (Currently Amended)   The method as claimed in claim 1, wherein ~~one user is assignable~~ the at least one role signature is a plurality of role signatures ~~simultaneously~~.

8.   (Previously Presented)   The method as claimed in claim 1, wherein the data

are medically relevant, wherein the users are medical specialist personnel, and

wherein the at least one role signature is formed in line with the workgroups within

the medical specialist personnel.

9.   (Currently Amended)   A data processing facility, comprising:

security check means for, prior to the data processing facility accessing

application data, performing a security check upon each access operation in order to

ascertain an identity of a user; and

a signature tool, ~~adapted~~ <u>configured</u> to assign a user signature, identifying the

user, on the basis of an output signal from the security check means without being

viewable by the user,

wherein the signature tool is ~~further adapted~~ <u>configured</u> to assign at least one

role signature, each role signature being assignable to a plurality of users <u>and</u>

<u>identifying a different activity group with a particular responsibility</u>, on the basis of an

output signal from the security check means without being viewable by the user,

[[and]]

~~wherein~~ the signature tool is ~~further adapted~~ <u>configured</u> to sign each access

operation to electronic data by specifying the user signature and the at least one role

signature, and

~~wherein~~ the signature tool is ~~still further adapted~~ <u>configured</u> to record each

access operation <u>by storing,</u> in an audit memory, <u>accessed application data</u>

<u>information and access operation information together with the user signature and the</u>

<u>at least one role signature specified for each access operation,</u> and record the user

signature in a user signature memory and in the audit memory, and record the at

least one role signature in a role signature memory and in the audit memory.

10.   (Original)   The data processing facility as claimed in claim 9, wherein the security check means is further for ascertaining biometric data from the user.

11.   (Currently Amended)   The data processing facility as claimed in claim 9, wherein the security check means is ~~adapted~~ configured to read at least one of electronic and mechanical keys.

12.   (Currently Amended)   The data processing facility as claimed in claim 9, wherein the signature tool has access to the user signature memory and is ~~adapted~~ configured to check the user signature memory, on the basis of an output signal from the security check means, for the user signature which is to be assigned.

13.   (Currently Amended)   The data processing facility as claimed in claim 9, wherein the signature tool has access to the role signature memory and is ~~adapted~~ configured to check the role signature memory, on the basis of an output signal from the security check means, for the at least one role signature which is to be assigned.

14.   (Original)   The data processing facility as claimed in claim 12, wherein the user signature memory is arranged remotely from the data processing facility, and wherein the signature tool has access thereto via a data telecommunication link.

15.   (Original)   The data processing facility as claimed in claim 9, wherein the data processing facility is a medical workstation.

16.   (Currently Amended)   A storage medium, ~~adapted~~ <u>configured</u> to store

information and ~~adapted~~ <u>configured</u> to interact with a data processing facility to

perform the method as claimed in claim 1.

17.   (Original)   The method as claimed in claim 2, wherein the security check

involves reading at least one of an electronic and mechanical key.

18.   (Previously Presented)   The method as claimed in claim 2, wherein the user

signature to be assigned is ascertainable on the basis of the data ascertained in the

security check, by checking the user signature memory.

19.   (Previously Presented)   The method as claimed in claim 3, wherein the user

signature to be assigned is ascertainable on the basis of the data ascertained in the

security check, by checking the user signature memory.

20.   (Previously Presented)   The method as claimed in claim 2, wherein the at

least one role signature to be assigned is ascertainable on the basis of the data

ascertained in the security check, by checking the role signature memory.

21.   (Previously Presented)   The method as claimed in claim 3, wherein the at

least one role signature to be assigned is ascertainable on the basis of the data

ascertained in the security check, by checking a role signature memory.

22.   (Original)   The method as claimed in claim 5, wherein the role signature

memory is checked using a data telecommunication link.

23-24. (Canceled)

25. (Currently Amended) The data processing facility as claimed in claim 11, wherein the signature tool has access to the user signature memory and is ~~adapted~~ configured to check the user signature memory, on the basis of an output signal from the security check means, for the user signature which is to be assigned.

26. (Canceled)

27. (Currently Amended) The data processing facility as claimed in claim 11, wherein the signature tool has access to the role signature memory and is ~~adapted~~ configured to check the role signature memory, on the basis of an output signal from the security check means, for the at least one role signature which is to be assigned.

28. (Original) The data processing facility as claimed in claim 13, wherein the role signature memory is arranged remotely from the data processing facility, and wherein the signature tool has access thereto via a data telecommunication link.

29. (Currently Amended) A data processing facility, comprising:

security check means for, prior to the data processing facility accessing application data, performing a security check upon each access operation in order to ascertain an identity of a user; and

signature tool means for assigning a user signature identifying the user, on the basis of an output signal from the security check means without being viewable by the

user, for assigning at least one role <u>signature, each role signature identifying a different activity group with a particular responsibility</u>, each role signature being assignable to a plurality of users, on the basis of an output signal from the security check means without being viewable by the user, for signing access operations to electronic data by specifying the user signature and the at least one role signature, and for recording each access operation <u>by storing accessed application data information and access operation information together with the user signature and the at least one role signature specified for each access operation</u> in an audit memory, recording the user signature in a user signature memory and in the audit memory, and recording the at least one role signature in a role signature memory and in the audit memory.

30. (Original) The data processing facility as claimed in claim 29, wherein the security check means is further for ascertaining biometric data from the user.

31. (Currently Amended) The data processing facility as claimed in claim 29, wherein the security check means is ~~adapted~~ <u>configured</u> to read at least one of electronic and mechanical keys.

32. (Previously Presented) The data processing facility as claimed in claim 29, wherein the signature tool means includes access to the user signature memory and is for checking the user signature memory, on the basis of an output signal from the security check means, for the user signature which is to be assigned.

33. (Previously Presented) The data processing facility as claimed in claim 29,

wherein the signature tool includes access to the role signature memory and is for

checking the role signature memory, on the basis of an output signal from the security

check means, for the at least one role signature which is to be assigned.

34.   (Previously Presented)   The data processing facility as claimed in claim 32,

wherein at least one of the user signature memory and the role signature memory is

arranged remotely from the data processing facility, and wherein the signature tool

has access to at least one of the user signature memory and the role signature

memory via a data telecommunication link.

35.   (Canceled)

36.   (Original)   The data processing facility as claimed in claim 29, wherein the

data processing facility is a medical workstation.

37-39.(Canceled)

40.   (Currently Amended)   A method for reconstruction of access operations to

electronic data, comprising:

        signing each access operation, wherein

                a security check is performed in order to ascertain the identity of a user,

                a user signature is assigned, identifying the user, on the basis of the

        performed security check, without being viewable by the user,

                at least one role signature is assigned, each role signature being assignable

        to a plurality of users, on the basis of the performed security check, without

being viewable by the user, <u>each role signature identifying a different activity</u>

<u>group with a particular responsibility,</u>

the access operation is signed by specifying the user signature and the at

least one role signature, and

each access operation and the user signature and the at least one role

signature specified for each access operation are recorded <u>by storing, in an</u>

<u>audit memory, accessed electronic data information and access operation</u>

<u>information together with the user signature and the at least one role signature</u>

<u>specified for each access operation,</u> wherein

~~each access operation is recorded in an audit memory,~~

the user signature is recorded in a user signature memory and in the

audit memory, and

the at least one role signature is stored in a role signature memory and

in the audit memory; and

reconstructing each access operation by specifying at least one of the user

signature and the at least one role signature and accessing the audit memory.

41.   (Previously Presented)   The method as claimed in claim 40, wherein an

access operation can be reconstructed by specifying at least one of the user's former

and current role signatures.

42.   (Canceled)

43.   (Previously Presented)   The method as claimed in claim 1, wherein the user signature memory and the role signature memory are maintained independently from the audit memory.

44.   (Previously Presented   The data processing facility as claimed in claim 9, wherein the user signature memory and the role signature memory are maintained independently from the audit memory.

45.   (Previously Presented)   The data processing facility as claimed in claim 29, wherein the user signature memory and the role signature memory are maintained independently from the audit memory.

46.   (Previously Presented)   The method as claimed in claim 40, wherein the user signature memory and the role signature memory are maintained independently from the audit memory.

*** END CLAIM LISTING ***